Claims

We claim:

1. A method of detecting a denial of service attack at a network server, comprising the steps of

counting the number of inbound packets and the number of discarded packets X in a specified interval,

if the number of discarded packets X in the interval exceeds a specified minimum X(MIN), then calculating the percentage of discarded packets R = X divided by the number of inbound packets, and

if R exceeds a specified threshold, then setting a denial of service event marker.

2. The method of claim 1 further comprising the step of collecting relevant inbound packet information to further characterize the attack.

3. The method of claim 2 wherein the step of collecting relevant inbound packet information further comprises

initiating a flood monitoring process that is executed at a specified intervals to collect the relevant inbound packet information while the attack is in progress.

4. The method of claim 3 wherein the flood monitoring process comprises

resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the process is lower than a specified minimum X(MIN2), wherein X(MIN2) may or may not equal X(MIN).

5. The method of claim 3 wherein the flood monitoring process comprises

resetting the denial of service event marker if the rate of discarded packets in the specified interval before execution of the process is less than a specified threshold.

6. The method of claim 4 or claim 5 comprising the further step of collecting relevant inbound packet information to further characterize the attack when is declared over.

7. The method of claim 6 wherein the collected packet information can consist of one or more of the following:

a) the number of inbound packets in the last interval;
b) the number of discarded packets in the last interval;
c) the packet discard rate;
d) the most frequent discard protocol type;
e) the most frequent discard discard type;
f) the media access control (MAC) address of the immediately prior packet hop.

8. The method of claim 3 wherein the flood monitoring process comprises

determining if the flood attack is still in progress by comparing the packets discarded in the last interval with the number of inbound packets, and

maintaining the scheduling of the flood monitoring process if the attack is still in progress.

9. The method of claim 8 further comprising collecting relevant inbound packet information for the last interval.